REMARKS/ARGUMENTS

Claims 1-5 were pending. Claims 1, 2 and 5 are amended herein and following entry of this amendment, claims 1-5 will be pending.

In an Office Action, the Examiner rejected claim 1 under 35 USC §102(b) as being anticipated by U.S. Patent No. 5,548,648 to Yorke-Smith and rejected claim 2 (and apparently claims 3-5 as well) under 35 USC §103(a) as being anticipated by Yorke-Smith in view of Koopman, U.S. Patent No. 5,619,575. Applicant respectfully traverses those rejections and requests reconsideration and withdrawal of the rejections for the reasons set forth herein.

Claim 1, as amended, is allowable over Yorke-Smith as that reference fails to disclose or suggest each element of claim 1. For example, the reference fails to disclose or suggest "using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first encrypted portion..." as claimed (underlining showing additions to the claim in this amendment). In making the rejection, the Examiner asserted that Yorke-Smith showed a second portion of a message overlapping a first portion of the message, identifying "transition regions" that constitute overlap regions. As explained in an earlier response, it is not clear that Yorke-Smith supports the Examiner's contention, but with a view to prompt allowance of the claims of the present application, claim 1 has been amended to clarify that a second portion of the message that is encrypted using the second key overlaps with a first encrypted portion (emphasis added). This reuse of an encrypted portion creates an authentication chain thus ensuring that the integrity of the chain is preserved and alteration is detected by a failed decryption.

Applicant submits that Yorke-Smith does not disclose or suggest that element. In fact, the source code included with the Yorke-Smith specification appears to indicate that each data block is processed on its own, without data overlapping from another data block, regardless of whether an encrypted portion is encrypted with a second portion. Therefore, for at least the reasons stated above, Applicant submits that claim 1 is allowable over Yorke-Smith.

Claim 2 was rejected over Yorke-Smith and Koopman. As amended, claim 2 is also allowable over those references they, alone or in combination, fail to disclose or suggest

each element of amended claim 2. For example, neither reference discloses or suggests the claimed encrypting subdivided fields using a first key to form cipher blocks, subdividing a designated cipher block into a cipher subblocks and encrypting a second of the cipher subblocks and the residual portion together with an authentication block using a second key to form a cipher residual block. As explained above with reference to claim 1, Yorke-Smith fails to show at least encrypting a block with a first key, combining the encrypted block with other blocks and encrypting using a second key.

Koopman was not cited as showing that lacking element in the references, nor was it cited to make up that deficiency of Yorke-Smith. Therefore, claim 2 and claims 3-4 dependent therefrom, are allowable over the cited references and the rejection should be withdrawn.

Claim 5, as amended, is allowable over Yorke-Smith and Koopman for similar reasons.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

Dated: 3/29/05

Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200 Fax: 415-576-0300
PHA:jtc
60307826 v1